IN THE CLAIMS

This listing of the claim will replace all prior versions and listings of claim in the present application.

Listing of Claims

Claims 1-8 (canceled).

9. (currently amended)A symmetric-key decryption method comprising the steps of:

dividing ciphertext to generate a plurality of ciphertext blocks each having a predetermined length;

generating a random number sequence based on a secret key;

generating a random number block corresponding to one of said plurality of ciphertext blocks from said random number sequence;

outputting a feedback value obtained as a result of operation on said one of the plurality of ciphertext blocks and said random number block, said feedback value being fed back ~~to~~ for use in the operation on another one of the plurality of ciphertext blocks; and

performing a decryption operation using said one of the plurality of ciphertext blocks, said random number block, and a said feedback value obtained as a result of operation on still another one of the plurality of ciphertext blocks to produce a plaintext block.

10. (original) The symmetric-key decryption method as claimed in claim 9, wherein said decryption operation uses one or more said random number

blocks whose total length is longer than a length of said one of the plurality of ciphertext blocks.

11. (original) The symmetric-key decryption method as claimed in claim 10, further comprising steps of:

concatenating a plurality of said plaintext blocks to generate plaintext;

extracting redundancy data included in said plaintext; and

checking said redundancy data to detect whether said ciphertext has been altered.

12. (original) The symmetric-key decryption method as claimed in claim 11, further comprising steps of:

extracting secret data included in said plaintext; and

checking said redundancy data and said secret data to detect whether said ciphertext has been altered.

Claims 13-20 (canceled).

21. (currently amended)A symmetric-key decryption apparatus comprising:

a circuit for receiving ciphertext, and dividing the received ciphertext to generate a plurality of ciphertext blocks each having a predetermined length;

a circuit for receiving a secret key to generate a random number sequence whose length is longer than a length of said ciphertext, and generating a random

number block corresponding to one of said plurality of ciphertext blocks from said random number sequence;

a circuit for outputting a feedback value obtained as a result of operation on said one of the plurality of ciphertext blocks and said random number block, said feedback value being fed back ~~to~~ for use in the operation on another one of the plurality of ciphertext blocks; and

a decryption operation circuit for performing a decryption operation using said one of the plurality of ciphertext blocks, said random number block, and a said feedback value obtained as a result of operation on still another one of the plurality of ciphertext blocks to produce a plaintext block.

22. (original) The symmetric-key decryption apparatus as claimed in claim 21, wherein said decryption operation circuit uses one or more said random number blocks whose total length is longer than a length of said one of the plurality of ciphertext blocks.

23. (original) The symmetric-key decryption apparatus as claimed in claim 22, further comprising:

a circuit for concatenating a plurality of said plaintext blocks to generate plaintext;

a circuit for extracting redundancy data included in said plaintext; and

a circuit for checking said redundancy data to detect whether said ciphertext has been altered.

24. (original) The decryption apparatus as claimed in claim 23, further comprising:

a circuit for extracting secret data included in said plaintext,

wherein said circuit for detecting whether said ciphertext has been altered checks said secret data and said redundancy data to detect whether said ciphertext has been altered.

Claims 25-32 (canceled).

33. (currently amended)A medium storing a program for causing a computer to perform a symmetric-key decryption method, wherein said program is read into said computer, said symmetric-key decryption method comprising the steps of:

receiving ciphertext, and dividing the received ciphertext to generate a plurality of ciphertext blocks each having a predetermined length;

receiving a secret key to generate a random number sequence whose length is longer than a length of said ciphertext, and generating a random number block corresponding to one of said plurality of ciphertext blocks from said random number sequence;

outputting a feedback value obtained as a result of operation on said one of ~~the~~said plurality of ciphertext blocks and said random number block, said feedback value being fed back ~~to~~for use in the operation on another one of ~~the~~said plurality of

ciphertext blocks; and

performing a decryption operation using said one of the plurality of ciphertext blocks, said random number block, and ~~a~~ said feedback value obtained as a result of operation on still another one of ~~the~~ said plurality of ciphertext blocks to produce a plaintext block.

34. (original) The medium storing a program as claimed in claim 33, wherein said decryption operation uses one or more said random number blocks whose total length is longer than a length of said one of the plurality of ciphertext blocks.

35. (original) The medium storing a program as claimed in claim 34, wherein said symmetric-key decryption method further comprises steps of:

concatenating a plurality of said plaintext blocks to generate plaintext;

extracting redundancy data included in said plaintext; and

checking said redundancy data to detect whether said ciphertext has been altered.

36. (original) The medium storing a program as claimed in claim 35, wherein said symmetric-key decryption method further comprises steps of:

extracting secret data included in said plaintext; and

checking said redundancy data and said secret data to detect whether said ciphertext has been altered.

Claim 37 (canceled).